PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD INDUSTRIAL DE SANTANDER

División de Servicios de Información
Universidad Industrial de Santander
Bucaramanga, Enero de 2024

Control de versiones del documento

Versión	Fecha	Responsable	Descripción
1	19/01/2021	División de Servicios de Información	Versión 1
2	19/01/2022	División de Servicios de Información	Versión 2
3	17/01/2023	División de Servicios de Información	Versión 3
4	30/01/2024	División de Servicios de Información	Versión 4

Tabla de Contenido

INTRODUCCIÓN

1. MARCO NORMATIVO
2. DEFINICIONES
3. OBJETIVOS
4. ALCANCE
5. PLAN DE ACCIÓN

Introducción

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el Mapa de Riesgos de Seguridad digital, con la combinación de zona de riesgo alta y extrema en el análisis del riesgo y evaluación del riesgo, evitando aquellas situaciones que impidan el logro de los objetivos de la Universidad Industrial de Santander - UIS.

El Plan de Tratamiento de Riesgos se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define la acción, el responsable y la fecha límite de realización, durante la vigencia 2024.

Las acciones identificadas se definieron teniendo en cuenta el análisis de riesgos, que brindó información acerca de las necesidades de seguridad de la información del Proceso Servicios Informáticos y de Telecomunicaciones de la Universidad, proporcionando las herramientas necesarias para definir cada una de las características de las medidas.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planeen acciones que reduzcan la afectación a la entidad en caso de materialización, adicional, se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados por la universidad.

1. MARCO NORMATIVO

- CONPES 3854 de 2016- Política Nacional de Seguridad Digital.
- Decreto 1008 - Lineamientos generales de la política de Gobierno Digital.
- ISO 27001:2013
- ISO 31000:2018

- Guía para la administración del riesgo y diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.
- Decreto 612 de 2018- Alineación de los 12 Planes al Plan Estratégico de la Institución.
- Guía del MinTIC de seguridad y privacidad de la información para la gestión del riesgo (guía # 7)
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas /MinTIC 2018.
- Manual para la administración del riesgo. MSE.01

2. DEFINICIONES

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio, evitando cumplir con sus objetivos.

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

3. OBJETIVOS

3.1. Objetivo General

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad digital a los que la UIS pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

3.2. Objetivos Específicos

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de seguridad digital y privacidad de la información, de acuerdo con los contextos establecidos en la Entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información y Seguridad Digital.

4. ALCANCE

El Plan de Tratamiento de Riesgo tendrá en cuenta como mínimo los riesgos que se encuentren en los niveles Alto y Extremo en la matriz de riesgos de seguridad digital de la Universidad. Acorde a los lineamientos definidos por la Universidad Industrial de Santander, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

En la Metodología de riesgos de seguridad digital de la Universidad, y en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1]: se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la UIS.

5. PLAN DE ACCIÓN

Item	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
1	Divulgar y socializar la política de seguridad de la información a las UAA involucradas en su cumplimiento.	División de Servicios de Información	30-nov-24	Registros de asistencia
2	Publicar y socializar el procedimiento de control de acceso físico a las instalaciones de procesamiento de información crítica.	División de Servicios de Información	30-jun-24	Procedimiento publicado y socializado
3	Solicitar al Comité Institucional de Gestión y Desempeño que se contrate y designe a un responsable de la Seguridad Digital institucional (ideal, que pertenezca a la planta de la universidad y pertenezca a la alta dirección).	División de Servicios de Información	30-jun-24	Solicitud enviada

4	Definir el plan de acción a seguir producto del análisis de vulnerabilidades realizado con RENATA.	División de Servicios de Información	30-jun-24	Plan de acción elaborado
5	Implementar múltiple factor de autenticación para las cuentas de correo electrónico funcionales de los jefes de unidad.	División de Servicios de Información	30-jun-24	Lista de cuentas de correo a las que se les activó el MFA.
6	Solicitar contraseñas de calidad para los correos electrónicos institucionales.	División de Servicios de Información	30-jun-24	Cambio implementado.
7	Socializar la importancia de los siguientes proyectos ante la alta dirección de la Universidad: 1- Adquisición de una solución de seguridad informática perimetral tipo NGFW para la red de datos LAN institucional. 2- Adquisición de solución WAF (Web Application Firewall) con balanceador de aplicaciones integrado	División de Servicios de Información	31-mar-24	Correo enviado - Socialización